1-1-2008

Data Model Development for Fire Related Extreme Events - An Activity Theory and Semiotics Approach

Rui Chen  
SUNY - Amherst, rc422@medaille.edu

Raj Sharman  
SUNY - Buffalo, rsharman@buffalo.edu

H R. Rao  
SUNY - Buffalo, mgmtrao@buffalo.edu

Shambhu J. Upadhyaya  
SUNY - Buffalo, shambhu@cse.Buffalo.EDU

Follow this and additional works at: http://aisel.aisnet.org/icis2008

Recommended Citation  
http://aisel.aisnet.org/icis2008/217

This material is brought to you by the International Conference on Information Systems (ICIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICIS 2008 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
DATA MODEL DEVELOPMENT FOR FIRE RELATED EXTREME EVENTS – AN ACTIVITY THEORY AND SEMIOTICS APPROACH

Développement d’un modèle de données pour les événements extrêmes liés au feu – une approche par la théorie de l’activité et la sémiotique

Rui Chen
Medaille College
Buffalo, NY 14214
rc422@medaille.edu

Raj Sharman
University at Buffalo
Amherst, NY 14260
rsharman@buffalo.edu

H. Raghav Rao
University at Buffalo
Amherst, NY 14260
mgmtrao@buffalo.edu

Shambhu J. Upadhya
University at Buffalo
Amherst, NY 14260
shambhu@cse.buffalo.edu

Abstract

Post analyses of major extreme events reveal that information sharing is critical for an effective emergency response. The lack of consistent data standards in the current emergency management practice however serves only to hinder efficient critical information flow among the incident responders. In this paper, we adopt a theory driven approach to develop a XML-based data model that prescribes a comprehensive set of data standards for fire related extreme events to better address the challenges of information interoperability. The data model development is guided by third generation Activity Theory and semiotics theories for requirement analyses. The model validation is achieved using a RFC-like process typical in standards development. This paper applies the standards to the real case of a fire incident scenario. Further, it complies with the national leading initiatives in emergency standards (National Information Exchange Model).

Keywords: Data model, standard, extreme event, activity theory, semiotics

Résumé

Le manque de standards de données dans la pratique actuelle de gestion des urgences réduit le flux efficient des informations cruciales entre les personnes chargées de répondre aux incidents. Dans ce papier, nous développons un modèle de données à base de XML qui prescrit un ensemble complet de standards de données pour les événements extrêmes liés au feu afin de mieux faire face aux défis de l’interopérabilité des informations. Le développement du modèle est guidé par la Théorie de l’Activité de troisième génération et par les théories sémiotiques.

Introduction

The 9/11 commission reports (Kean 2004) as well as analyses of Hurricane Katrina (Townsend 2006) have documented the inadequacies of response management. Among the factors accountable for the observed inadequacy, communication interoperability has been recognized for its critical role in supporting an effective response (Aylward et al. 2006; DHS 2005). Interoperability refers to the ability of two or more entities or systems to exchange information and to use the information that has been exchanged (IEEE 1990). Communication interoperability is crucial to inter-organizational communications among response agents (e.g., local, state, and federal) and it enables...
the multi-agent collaboration and coordination. There exist a number of emergency data standards addressing
general interoperability issues. However, they are not adequately designed to address day-to-day incidents such as
fire. Figure 1 (a real fire response document) captures some of the information that may be shared during a typical
fire incident. Even the leading national data standard for emergency management, National Information Exchange
Model (NIEM) (DHS et al. 2006), does not currently support many of the elements needed for such incidents. The
lack of emergency data standards can cause ambiguity and misinterpretation when information is exchanged among
responding parties (Chen et al. 2008a; Rao et al. 1995).

<table>
<thead>
<tr>
<th>Example Data Element</th>
<th>NIEM Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extent of Damage</td>
<td>No Support</td>
</tr>
<tr>
<td>Construction Type</td>
<td>No Support</td>
</tr>
<tr>
<td>Sprinkler Performance</td>
<td>No Support</td>
</tr>
</tbody>
</table>

Figure 1. Example Document Used for Fire Incident Response

In this paper we develop a data model for fire incident response. Fire incident is one of the most common incident
types and it causes significant amount of loss each year (Karter 2006). The data model development process
employs third-generation activity theory for requirement solicitation and semiotics theories for requirement analysis.
This paper makes two major contributions. First, it presents a new data model development methodology that is
based on third-generation activity theory and semiotics theories. Second, it develops and validates an object-oriented
XML data model to support real-time response information exchange during fire incident response.

This paper is organized as follows. We first examine existing literature on emergency data interoperability, Activity
Theory, and Semiotics. We then present the new data model development methodology. Next, we elaborate the
details of the fire response data model. We further present a case illustration to evaluate the data model usability.
Finally, we discuss the paper’s implications, limitations, and directions for future research.

Theoretical Foundation

Emergency Interoperability

Emergency response organizations’ existing response information systems are somewhat fragmented, localized, and
technologically disconnected (Frale 2005; NIEM 2006). The heterogeneity of the systems typically cause
communication interoperability and interrupt the information flow. Even among similar organizations such as fire
companies, the way that information is shared and managed may vary from county to county (Chen et al. 2007).

Given this realization, the U.S. Department of Homeland Security has allocated $280 million specifically to address
the ability of fire, emergency medical service, and law enforcement personnel to communicate with each other
across disciplines and jurisdictions (DHS 2005). The national efforts in emergency communication interoperability
can be found in the following literature: (BJA-DOJ 2003; CDC 2004; COMCARE 2002a; EIC 2004; HL7 2003;
IEEE 1997; LEITSC 2006; NEMSIS 2005; NENA 2000). They cover domains of law and public safety, emergency
management, transportation, emergency medical service, medicine, and public health.

The foundation for communication interoperability is data level interoperability which establishes a common
semantic understanding among participating organizations and also ensures that data is formatted in a semantically
consistent manner (Jump et al. 2003). A number of emergency related data standards have been developed by the
public and private sectors (COMCARE 2002b; DHS et al. 2006; DOJ 2005; E9-1-1 2006a; E9-1-1 2006b; EIC
progress towards an emergency data standard has been achieved by the leading national efforts: the GJXDM and
NIEM projects. The GJXDM, initiated by DOJ, defines a complete set of data standards for the field of Justice and
public safety. It consists of a well defined and organized vocabulary of over 2,500 reusable components, of which
600 are data types and over 2,000 are properties that facilitate the exchange and reuse of information from multiple sources and applications (Office of Justice Programs 2005). The NIEM project was initiated to further the success of GJXDM in unifying information exchange standards across a broader array of domains. The latest NIEM package is a collection of 828 data types and 4090 data properties for nine domains, including emergency management (DHS et al. 2006). The existing set of NIEM data standards for emergency management is narrowly defined around alarm event, resource, and message distribution. With regard to the complexity and diversity involved in the emergency management, a great amount of information is missing for day-to-day emergency operations and large scale multi-hazard incidents. The lack of information standard support weakens information sharing capabilities and consequently, such a lack also weakens response capabilities. In this paper, we develop a data model to standardize the task critical data to be shared and exchanged during fire incident response.

Activity Theory

The development of data model requires systematic approaches to elicit and analyze the internal elements, structure, and relationships of core data elements (Zowghi et al. 2005). In this paper, we use Activity Theory to guide the requirement engineering process in data standard development (Engestrom 1987; Engestrom 1999). An approach driven by Activity Theory represents a method that has gained increasing attention in recent years (Chaudhury et al. 2001; Kaptelinin et al. 2006; Uden et al. 2007). Activity Theory provides a lens to analyze the computer-supported activity of a group or organization and to study the design of artifacts for individuals and organizations.

Activity Theory suggests that human activity is directed toward a material or ideal object, mediated by artifacts or instruments, and socially constituted within the surrounding environment (Bertelsen et al. 2003; Vygotsky 1978). Activity can be understood as a systemic structure with various activities that are collated or extended away from the core activities (Bertelsen et al. 2003). The subject is the active element of the process and can be either an individual or a group. The object transformed by the activity can be an ideal or material object (Fuentes et al. 2003). The transformation process is enabled and supported by instruments (physical or logical). The instrument provides the subject with the experience historically collected by his/her community (Fuentes et al. 2003; Webb et al. 2006). During the interaction, subjects internalize and/or externalize their cognitive schemes and their understanding of the relationship between themselves and the external objects, instruments, surroundings, etc. Activity Theory also considers contradictions as one critical aspect and suggests that contradictions are the driving force in human interaction and system design (Bertelsen et al. 2003; Uden et al. 2007). The contradictions may also exist in the subjects, objects, instruments, and their interactions. In Activity theory, activity is constantly developing as a result of contradictions and instability and because of the development of new needs.

Activity theories have currently evolved to the third-generation. The first generation Activity Theory is focused on individual action and it studies subject, mediating artifact (instrument), and object only. The second generation Activity Theory is focused on collective activity and it studies a single activity system including subject, instrument, object, rules, community, and division of labor. The third generation Activity Theory employs multiple interacting activity systems to investigate the complex phenomena under question. It thus provides more refined and detailed accounts of the embedding issues and critical concerns of the research topic. To investigate the complex phenomena of emergency response and information sharing, in this study, we apply the third generation Activity Theory to elicit the requirements for data model development.

The concepts of Activity Theory have significant implications for our study. Emergency response involves complex networks of actors, resources, and operations. The intra-organizational, inter-organizational, and environmental interactions take place at high velocity. Emergency response also undergoes frequent restructuring with existing elements (e.g., actors and resources) removed, new elements introduced, and relationships altered. Applying Activity Theory, we investigate the emergency response along dimensions of subject, activity, instrument, activity, community, rule, and division of labor. The Activity Theory helps identify the focal interest of the research and formalize the requirement engineering processes to be followed. In the later section of the paper, we illustrate by examples how Activity Theory facilitates the requirement engineering. We also extend the traditional formalisms of Activity Theory (Engestrom 1987) to include “environment” as a relevant and important construct. Environmental factors (e.g., environmental hazards, threats, and weather) impact the activities carried out by subjects.
**Semiotics Theory**

Activity Theory approach captures the core data elements and their internal structures. To design the data model for higher efficiency in conveying meaningful information, we adopt semiotics to facilitate the data model development. Humans employ both tangible (e.g., signs) and intangible (e.g., norm) symbols to construct, maintain, and communicate meanings. The study of symbols and how they portend for processes like conflict and control allows us to better understand interpersonal and inter-organizational communication and to develop the emergency data model accordingly. Semiotics theory offers an approach for interpreting and making sense of meanings undergird organizational communication. Semiotics can be defined as the domain of investigation that explores the nature and functions of signs as well as the systems and processes underlying the signification, expression, representation and communication of the signs (Gorden & Kreiswirth, 2005). Like the symbolic interactionists, semioticians assume that our relationship with the physical and social world is mediated by symbolic processes. Like ethnomethodology, semiotics concerns pragmatics, the investigation of rules of use by which communications are produced and interpreted (Barley 1983). Semiotics is therefore ultimately the study of how communication is possible and it has been applied in studies of information system evolution (Desouza et al. 2002), information system classification (Barron et al. 1999), and information system ontology (Stamper et al. 2000).

At the core of semiotics is the notion of the sign. A sign is understood to be the relationship between or the union of a sign-vehicle (an expression or form such as a word, sound, or colored light) and the signified, the notion or content conveyed by the sign vehicle (Barthes, 1967). The link between expression and content is arbitrary in the sense that it is a convention of the group to which the sign's users belong. Arbitrary coupling implies that the same expression can signify alternative contents and those similar contents can be conveyed by different expressions, depending on the conventions one holds.

Peirce suggests that semiotics involves a triadic relationship between the representamen, object, and interpretant (Peirce 1931). The representamen is the physical signal or sign created to represent the object. The object is the meaning or understanding attached to the sign by its creator. The interpretant is the understanding or meaning created in the mind of the perceiver of the sign. The semiotics model posits that the nature of the sign is that there may be a mismatch between the object and the interpretant, e.g. the understanding of the developer and that of the user (Evermann et al. 2007).

The concepts of semiotics have significant implications for our study. During the data model development process, developers may create artifacts, such as symbolic icons, as signs in order to mitigate the potentials of mismatch between the developers and the data model users. Chandler defines symbolic icons as a language in which the signifier does not resemble the signified but which is fundamentally arbitrary or purely conventional (Shandler 2002). Examples of symbolic icons are the stop sign and the traffic light. Sign-based language such as symbolic icons has more effect than non-sign-based one as the former is more motivated and requires less amount of learning. By using symbolic icons, data model developers may create a data system that readily arouses correct and consistent denotation and connation among the users, as compared with cases with non-sign-based approaches. In the study, we develop symbolic icons in the data model for meaningful communication at efficiency.

**Data Model Development**

To support information sharing during a response to fire incident, we develop a XML-based data model. We apply the third-generation Activity Theory and semiotics theory in data model development.

Emergency response to fire incident typically consists of an onsite response entity and a remote management entity such as emergency operation center (EOC). Onsite response is usually reactive and the time window for incident mitigation is small. We characterize this as the “Mini-Second Response.” It is characterized by working with the local picture stemming from the local scenario. Without a proper understanding of the global picture, actions are motivated as a reaction to incidents from the immediate scene. Meanwhile, a supervisory structure such as EOC deals with more strategic issues and works with a global picture, leveraging external resources to help the onsite response. The actions of the EOC emanate based on a more reflective and proactive posture and the EOC commanders typically operate with a large time window. We classify such management efforts as “Many-Second Response.” The concepts of mini-second and many-second management cycle relate to distinct response tasks (operation- vs. strategic-level); constraints (small vs. large time window, information/intelligence and capability);
and outcome quality (poor vs. good) (Chen et al. 2008b). Mini-second response addresses immediate mitigation needs while many-second response oversees and supports the former, for instance with resources and information.

Through the third generation Activity Theory, we examine the emergency information sharing in the two activity systems mentioned above (See Figure 2). The lens of Activity Theory allows us to gain in-depth understanding of the social and technical systems and to elicit requirements for data standard development.

![Diagram](image)

**Figure 2. Application of Third-Generation Activity Theory on Data Model Development**

In Table 1 we map the third-generation Activity Theory concepts in the context of fire incident response. We provide only an illustrative set of guidelines generated from the third-generation Activity Theory as servers the intent of explicating the applicability of the theory and further allows us to also observe page restrictions on the manuscript.

<table>
<thead>
<tr>
<th>Activity Theory Concept</th>
<th>Mini-Second Response</th>
<th>Many-Second Response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition</td>
<td>Individual onsite responders who provide immediate mitigation to the fire incident</td>
<td>Individual response organization principals, supportive agent representatives, and emergency managers</td>
</tr>
<tr>
<td>Design Implication</td>
<td>The subjects involved in mitigation need to be identified so as to learn their individual experience and viewpoints that are operation-oriented</td>
<td>The subjects involved in supervision need to be identified so as to learn their individual experience and viewpoints that are management-oriented</td>
</tr>
<tr>
<td><strong>Object</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition</td>
<td>Local information flow that goes between onsite responders for tactical collaboration</td>
<td>Global information flow that goes in and out of the EOC, connecting onsite, local, and regional response services for strategic coordination</td>
</tr>
<tr>
<td>Design Implication</td>
<td>The data standard should be concise to reduce communication cost and effort; but also comprehensive to serve the information needs</td>
<td>The data standard shall be readable by all the participating organizations. This prompts the use of XML in describing the data model</td>
</tr>
<tr>
<td><strong>Community</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition</td>
<td>Core emergency services such as fire and rescue, law and order, and emergency medical personnel, hazmat teams, etc</td>
<td>Supportive emergency agencies (regional, state, and federal) and organizations (NPO, private, and public)</td>
</tr>
<tr>
<td>Design Implication</td>
<td>The data standard should consider the different perspectives (e.g., daily routine and expertise) each sub-community brings in. Also consider the perspective differences within sub-community (e.g., among fire companies)</td>
<td>Requirements should be elicited from multiple municipalities and across local, state, and federal hierarchy. We’d also consider the differences in information artifacts they currently adopt</td>
</tr>
</tbody>
</table>
We develop a number of symbolic icons to facilitate the information processing of the artifacts (i.e., data type and elements) of the data model. Examples of symbolic icons are in Table 2.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Data Element</th>
<th>Definition</th>
<th>Symbolic Value</th>
</tr>
</thead>
</table>
| OnsiteMaterial   | OnSiteMaterialFireLoad| A description of the extent to which the material may burn                 | *Green*: non-ignitable  
*Yellow*: intermediate degree of ignitability  
*Red*: highly ignitable |
| CivilianCasualty | HealthCondition       | A description of the health condition of the civilian victim              | *Green*: minor injuries; walking wounded  
*Yellow*: intermediate injuries  
*Red*: critically ill |
| FireServiceCasualty | HealthCondition     | A description of the health condition of the civilian victim              | *Green*: minor injuries; walking wounded  
*Yellow*: intermediate injuries  
*Red*: critically ill |
| Structure        | StructureSafety       | A description of the structure / building safety condition                | *Green*: structure unaffected; safe for entry  
*Yellow*: caution to exercise  
*Red*: not safe for entry, e.g., the house is likely to collapse |
<table>
<thead>
<tr>
<th>Location</th>
<th>Parameter</th>
<th>Description</th>
<th>Safety Condition</th>
</tr>
</thead>
</table>
| IncidentSpecifics | AlertLevel | A description of the alert level of the incident | Green: green zone; incident is mitigated or nearly mitigated exposing no threat  
Yellow: incident under control  
Red: hot zone; incident keeps escalating |

**Data Model Development Flow**

In this section, we introduce the development process of the fire incident response data model. The data model is integrated with a data dictionary in order to achieve semantic consistency for the standardization; the data dictionary is a well-defined vocabulary of data types, elements, and definitions of response-related elements. Further, the data model maintains structural consistency by following object-oriented design and by enforcing rule structures in the form of dictionary schemas.

**Initial Development**

We start the model development with a document collection process: we collected documents and notes from first responders who had a significant amount of expertise and experience in responding to extreme events relating to fire and incident response communication. This collection provided us with an idea of the kind of task-critical documents/publications that are used for information sharing in responding to a fire incident. During this process, over 40 documents were analyzed. These documents include fire incident response technical data forms; fire incident response dispatch forms; field notes and chronological logs; fire incident messaging systems (e.g., National Fire Incident Reporting System-NFIRS (DOS et al. 2006)), and fire response plans. They provide a systematic foundation for the data model development.

Next, we extract the response task-critical data from the various documents by examining the document fields and the context of usage. We first identify the data taxonomy for the response-critical information used in a typical fire response. Second, we define the data structure by analyzing this data taxonomy with regard to business contexts, purposes, usages, and users. The set of data elements are divided into groups where relevant elements form distinct data types. In addition we define data elements, data constraints and rule structures in this step.

Then, we define the “data typing” of identified data components. As discussed before, there are a number of emergency data standards. We choose the NIEM data standard as the foundation for the new data model for two reasons; first, NIEM standards define a set of elementary vocabulary for emergency response management and second, NIEM standards are organized through object-oriented structures. Object-oriented structure ensures the model consistency and they facilitate the development of new data types through inheritance and extensions.

The response data model mediates not only information sharing but also the collaborative situational awareness and coordination among the response agents (Rao et al. 1995). To this end, we employ XML to specify and record the fire response data model. Where the response agents are concerned, XML-based dictionary specification allows the platform-interdependent utilization of data standards and the development of automated information processing tools via heterogeneous technological solutions (DOJ 2005; March et al. 2000; Mendling et al. 2006; W3C 2000). This support to agency collaboration and coordination is also facilitated through NIEM in that it is going to be propagated national wide, cross Federal, State, and local levels, as U.S. emergency response data standard.

**Data Model Validation**

Our data model is validated by domain experts who evaluated the model and provided feedback (Boudreau et al. 2001; Jakobs et al. 1998). The validation process includes four fire expert evaluators (18 years of fire experience on average). The evaluators are experienced with the fire incident response and information sharing practices and their knowledge helped identify and address the potential problems with the use of data model in practice.
The evaluators are individually contacted for their review feedback. To facilitate validation, we also develop a request for comment (RFC) (Wikipedia 2006b) document to introduce the research project to the evaluators. This RFC document outlines the research objectives, development process, and proposed data model. The authors conduct onsite visits (two per evaluator) and have email contact with the evaluators to distribute the RFC and collect the feedback. The evaluation generate over 30 non-overlapping comments relating to coverage, depth, logic, organization, and naming. Next, with the help of the evaluators, the authors modify the data model to incorporate the feedback. This modification results in major changes to 9 data types in addition to around over 20 other changes. The data model has in itself over 50 data types, over 180 data elements, and over 70 codes. In addition, it utilizes three external data coding schemes. Complete data model specification spreadsheet and XML schema (over 30 pages) are available upon request.

We present a snapshot of the fire response data developed in Figure 3 which illustrates the major data dimensions and components. The data model is important to construct the incident reports, dispatch forms, assessment reports, response plans, situation reports, request forms, comments, response summaries etc. We also number, arbitrarily, the individual data model components in Figure 4 to allow us cross reference them in later sections. In the next section, we describe the details of the data dictionary in which the data components are formally defined and typed.

**Data Model Description**

We introduce the data model developed for fire response information sharing. For the sake of concision, we present only few examples of the data types and elements in the new data model. The full elaboration of entire data model is available upon request.

**Threat Assessment**

Threat assessment is an important response task in which response agents analyze the incident situation to make an informed decisions and decide on the nature of their strategic response.

**Incident Setting Vocabulary**

Timely sharing and exchange of incident setting data provides the responders with a quick overview of the incident. Example of the incident setting vocabulary includes the `incident specifics` type which presents the basic information on fire incidents. Its data elements include `incident ID, description, fire category`, and both date and time of `incident start, alarm, under control, overhaul, and end`. To this end, we develop a data type “IncidentSpecificsType.” As some incident specifics elements are defined in NIEM `u:ActivityType`, we establish an inheritance relationship between the two. Following NIEM alike “Object-Oriented” design, the proposed `IncidentSpecificsType` is designed to inherit from `u:ActivityType`. This allows it to inherit and reuse all the data elements in the latter without redefining them. New elements (such as `alarm date` and `alarm time`) missing from `u:ActivityType` are added into the `IncidentSpecificsType` to support fire response. Other important data types of incident setting include `incident location`, `weather`, and `building structure` type.

**Fire Hazard Data Vocabulary**

During the response to a fire incident, the sharing of information on fire hazards allows the responders to comprehend the potential hazards that may emerge. To this end, we have developed two data types: `FireBehaviorType` and `HazardFactorType`. The `FireBehaviorType` describes the real-time fire development and trend of progress. Key elements are such as `fire fuel, fire heat, fire oxygen` which are necessary ingredients required for a fire, also referred to as “Fire Triangle” (NIFC 2006; Wikipedia 2006a). In addition, fire behavior data includes element such as `fire spread, rate of spread, flame length`, etc. It is important for the incident commanders to comprehend these pieces of information before an effective response plan can be designed and operation safety be ensured. The `HazardFactorType` on the other hand is designed to capture the set of fire hazard factors present. These hazards may directly or indirectly contribute to the fire escalation. Fire hazards include factors from `building construction` (e.g., wall collapse), `act or omission` (e.g., fire door blocked), `on site materials` (e.g., explosive hazard..."
material), delay (e.g., delayed detection of fire), etc. A close monitoring of the hazard factors should be implemented as to detect and predict any emerging hazards.
Figure 3. Fire Response Data Model Overview

(Major data components are arbitrarily numbered to allow cross reference)
Fire Threat Data Vocabulary

Information on threats reveals the immediate consequences resulted due to the fire. Fire incidents may cause consequences such as personal injury and casualty, chemical release and environmental contamination, property damage, and public safety impact. We have developed a number of data types, including casualty type, civilian casualty type, fire service casualty type, property damage type, and environment damage type.

Incident Command System

The data vocabulary for incident command system captures the response management design and response operations. During the course of response, it is important to immediately publish information on the incident command system in place as it provides situational awareness of the collective response, clarify the task assignment and resource allocation, and enforce the command and control.

Response Management Data Vocabulary

We follow the guidelines provided by the national incident management system (NIMS) to identify major data components such as response facility, incident command system (ICS), response organization and response resources. NIMS defines “responder” as one type of resource in general; in this data model, however, we differentiate responders from other resources (e.g., fire engine) as responders are complex entities that may assume management roles and harness the other resources to carry out response tasks.

Response Operations Data Vocabulary

We also develop data vocabulary for response operation. The standard for such information facilitates the monitoring, tracking, and analysis of response progress, ensuring that the mitigation develops as designed. Example data type is ResponseOperationPlanType which describes the detailed response plans. An incident response may have multiple plans designed at varying stages of the response life cycle. Example response plan elements include plan name, ID, plan objective and plan evaluation.

Table 3 provides a sample list of data model elements derived from Activity Theory and semiotics. It illustrates how the design implications listed in Table 1 and Table 2 are incorporated into the data model development.

<table>
<thead>
<tr>
<th>Table 3. Examples of Theory Informed Data Model Components</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Model Artifact</strong></td>
</tr>
<tr>
<td>On Site Material (Figure 3: component 7)</td>
</tr>
<tr>
<td>On Site Material Fire Load</td>
</tr>
<tr>
<td>Civilian Casualty (Figure 3: component 13)</td>
</tr>
<tr>
<td>Health Condition</td>
</tr>
</tbody>
</table>

Case Illustration of Data Model Application

We apply the data model to a real document exchanged during fire incident response. The application demonstrates the effect of the data model on real-life emergency management. It further presents a typical process in which the data model may be utilized to leverage the existing response capabilities by resolving interoperability breakdowns and enhancing information availability and quality. The document we study is titled “Fire Report Form.” This form
and similar others are used in Western New York and are exchanged between local fire agencies and the New York State for the reporting of fire incident management.

To standardize the Fire Report Form using our data model, we follow a process that resembles the NIEM Information Exchange Package Development style. The three phases - namely Modeling, Mapping, and XML Instance Building - transfer the unstructured and un-standardized paper documents into a syntactic, structured, and semantically homogeneous XML document. This transfer allows for automatic processing by end-user computer systems and enables easy importing and exporting to share response critical information.

The modeling process analyzes the document content and structure. For the Fire Report Form, we present the document domain model in Figure 4. The domain model categorizes and groups the document fields according to their relevance. For example, the document fields such as smoke detector, detector operable, and battery or A/C together describe the detector information. We therefore group these document fields together (as in composition operation in Object-Oriented Modeling) and create a domain entity named Detector. Following this strategy, the entire Fire Report Form is divided and represented by a set of domain entities.

Based on the domain model, we map the document fields into the data standards in the fire response data model and NIEM. The mapping results are recorded and a snapshot is illustrated in Figure 5a. For example, the domain entity of Detector is mapped to FireDetectorType in the fire response data model. This mapping thus allows the related document fields to be mapped to corresponding data elements in the FireDetectorType. All the document fields are mapped into fire response data model. The mapping reveals its great level of usefulness and flexibility in meeting the standardization requirements. The mapping process is followed by the XML instance creation process. We develop a XML document (see Figure 5b) which allows the emergency responders to distribute it with others. In this way, the data model standardizes the unstructured paper based document into standardized XML document for timely sharing and processing on emergency response computer systems.

Figure 4. Domain Model of Fire Report Form
Discussion and Conclusion

Information interoperability is a key component to the information sharing and exchange in an emergency response. Standards are important not only for human interoperability but also device interoperability such as communication between sensors and first responder handheld devices. In this study, the authors propose an object-oriented XML data model for fire incident response. The data model in this paper provides consistent semantics to describe the response information and ensures information interoperability. The design and development adheres to the principles enunciated in the literature on design science (Hevner et al. 2004; March et al. 1995). For instance, problem relevance stems from the fact that we are focusing on fire incidents and response information interoperability issues (DHS 2005; Harrison et al. 2006; Weinshel 2006). The research design is grounded on emergency practices and is supported by those in the emergency community who have collaborated in this exercise to ensure the usefulness and quality of our data model. The data model is developed by performing a thorough analysis of the requirements of response information management and by identifying an extensive amount of response data provided by response stakeholders and response information systems. There are three clearly identifiable artifacts produced in this research. First, a comprehensive data vocabulary for fire incident response is designed. Second, the object-oriented dictionary structure is developed to ensure its internal consistency and to allow for future extension. Third, the XML-based data dictionary schema is delivered as a data model specification. It enhances the data model usability by allowing the platform to have interdependency, design of automation tools,
and information validity verification. Finally the data model is validated by a panel of domain experts in fire response; further, an illustration of the data model is presented which exemplifies its usability and usefulness in addressing practical issues in the field.

This data model is generalizable to other incident types. As in Figure 3, the data model consists of components that may standardize information sharing in response to other incident scenarios. These data components include incident specifics, response management, and response operation and they are commonly used in many other incident scenarios. The data model also consists of components that are scenario-specific including fire hazard and threat. To develop data model for other incidents such as earthquake, these data components may be replaced with hazard and threat pertaining to the specific incident scenario under question. For example, a data model for earthquake may include earthquake hazard and threat data elements while keeping all other data elements.

Limitations and Future Research

This study has certain limitations. First, the data model may not comprehensively address all aspects of the information sharing requirements during fire incident response. Second, the data model development relies primarily on the response documentation collected from the emergency response community of Western New York. Future extension includes collecting data from first responders in California to include data items from forest fire incidents as well.

The limitations also serve as directions for future research and development. The fire response data model provides a systematic overview of the required key response information. Future research, therefore, may include the development of expert systems for emergency information management. Incidents of all types share key information such as incident setting and response management; thus, the existing data model may be reused and extended for other incident types. Future research may generalize the existing data model for generic incident response and develop data models for other incident types such as nuclear incidents, severe snow storms, etc. Future research may also develop response performance metrics on the basis of threat assessment and incident command system information. Additional future research may develop an emergency index (e.g., Bayesian algorithms) on the basis of the individual symbolic codes of emergency facts. For example, a red code may be generated to indicate an escalating incident when a combination of response symptoms is present; multiple agencies will be brought into incident response. Otherwise it goes to green; the supportive agencies can be released to attend other fires and not tie up resources.

To conclude, the lack of consistent communication data standards for emergency management is an impediment to an efficient information sharing and exchange in the context of emergency response systems that cater to specific emergencies such as fire, severe snow storms, etc. In this paper, we provide a review of the national efforts toward creating emergency response management data standards. Using fire incidents as an example, the paper develops a systematic data model to capture and standardize response-critical information for fire incidents management. The paper provides a detailed data model along with a data dictionary and an object-oriented structure. This project is among the first attempts in the response community to propose solutions that contribute to the creation of an ultimate set of emergency data standards. The fire incident data model improves collaboration and information sharing among response organizations and agencies.

Acknowledgement

The authors would like to thank the SE, AE and referees for insightful comments that have greatly improved the paper.

This research is supported by NSF under grants 0802062 and 0809186. The usual disclaimer applies.
Reference


DOJ "Building Exchange Content Using the Global Justice XML Data Model," Department of Justice, Washington, DC.


NIEM "NIEM Concept of Operations," [www.niem.org](http://www.niem.org), Washing, DC.

NIFC "This Thing Called Fire," National Interagency Fire Center, Boise, Idaho.


PHIN "PHIN Vocabulary Standards and Specifications," Center for Disease Control and Prevention, 2005.


W3C "Extensible Markup Language (XML) 1.0," W3C, [http://www.w3.org/TR/REC-xml](http://www.w3.org/TR/REC-xml).


Weinschel, K. "UTC Promotes Emergency Response Interoperability," The United Telecom Council Washing, DC.

